

WHITE PAPER.

Pharmaceutical trade and the FDA anti-counterfeiting guidelines: Easy money and hard targets

Without more effective deterrents, counterfeiting will create a global crisis of confidence in the life sciences industry. With new drug development requiring an average of 12 years and \$1.7 billion, improving measures to combat counterfeiting should be viewed as guarding a strategic investment. The FDA's initial guidelines for pharmaceuticals are stimulating vigorous investigation by industry partners and will have broad strategic and operational implications. What is the right response for life sciences organizations looking to maximize security and optimize supply chain performance?

- > Consulting.
- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.

UNISYS

Imagine it • Done •

PHARMACEUTICAL COUNTERFEITING: EASY MONEY & HARD TARGETS

A white paper for life sciences executives.

Abstract.

In response to the proliferation of counterfeit medications, the U.S. Food and Drug Administration (FDA) recently issued guidelines intended to increase consumer safety by hardening the pharmaceutical supply chain. The guidelines are a likely precursor to regulation requiring pharmaceutical manufacturers and their trading partners to adopt radio frequency identification (RFID) technology to verify the authenticity of drugs and track and trace every item in their supply chains, from the point of origin to the point of sale to consumers. Beyond satisfying the FDA and reducing the counterfeiting threat, pharmaceutical organizations that adopt RFID can generate significant operational and financial benefits in inventory management, order accuracy and overall supply chain performance. To realize these gains, however, they must leverage experiences from prior RFID-based implementations and apply business intelligence and integration tools that can transform the explosion of electronic product code (EPC) data into actionable information.

The scope of the challenge.

Counterfeiters are organized criminals who exploit blind spots in the pharmaceutical supply chain for profit. They tend to operate as decentralized groups. Some groups have insider relationships at smaller distributors near the point of transfer to the consumer. They focus on selling the fake drugs. Other groups have access to the raw and packaging materials and focus on creating fakes. These groups can operate domestically or far outside U.S. borders and often have deal-driven relationships that change frequently. They represent “hard targets” for companies and agencies looking to stop them. Due to the amorphous nature of the threat, no single measure — not even electronic pedigrees — can provide adequate protection from counterfeiting.

Concerned by this rapidly growing problem, the FDA assembled a Counterfeit Drug Task Force in July 2003. The team of government, industry and technology experts recently issued its initial report, which contains specific guidelines for improving supply chain security and consumer safety. The FDA’s involvement reflects the significant threat to American consumers and corporations posed by the increasing sophistication of counterfeiters and the emergence of “gray markets.” Once thought to be a problem only in developing countries, several sobering incidents have clearly demonstrated the growing threat to the U.S. drug supply. However, much of the counterfeit medicine uncovered by authorities originates outside the borders of the U.S. Consider that:

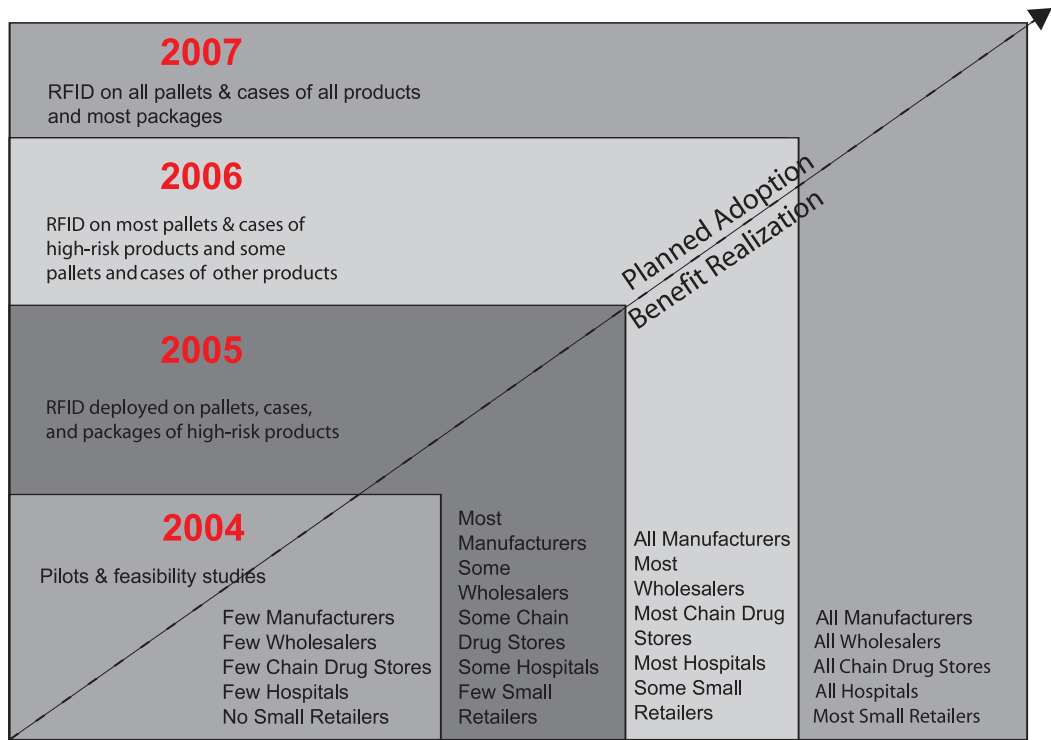
- ▶ The World Health Organization estimates that between five and 10 percent of world pharmaceuticals are counterfeit, with as much as 25 percent in Third World markets;
- ▶ In inspecting 1,153 shipments of drugs into the U.S., the FDA and U.S. Customs and Border Protection (CBP) recently found that 88 percent contained unapproved and potentially harmful goods;

- ▶ China is considered by the U.S. Customs department to be, by far, the worst offender of exporting counterfeit products;
- ▶ Counterfeit Viagra, most of it of Chinese origin, has been discovered in every corner of the globe, including the U.S., Mexico, the Middle East, Russia and Southeast Asia;
- ▶ More than 200,000 bottles of counterfeit Lipitor have been found in the U.S. over the past three years, with many of the copies so convincing that they escaped detection for months.

Due to the amorphous nature of the threat, no single measure — not even electronic pedigrees — can provide adequate protection from counterfeiting.

Today, the industry doesn't know what it doesn't know. Reliable data on occurrences of counterfeiting is hard to find. It's no surprise that estimates on the impact of counterfeiting vary widely — from \$1 billion to \$12 billion. The recent FDA guidelines are a call to action for the industry to explore better ways to combat counterfeiting. The FDA's report includes specific recommendations for deterrence. Among other steps, the FDA is recommending that pharmaceutical manufacturers work with their trading partners to improve supply chain visibility by attaching RFID tags with EPCs at the pallet, case and package level. The goal is to enable "instant verification" and rapid location of every item in the supply chain. The guidelines direct pharmaceuticals to develop track and trace capabilities. That is, companies must implement EPC-based systems that allow them to maintain an electronic record or "pedigree" of all the transactions involving the product as it flows through the pipeline. This is commonly referred to as "mass serialization." In the short term, the FDA is encouraging organizations to start pilots to determine the feasibility of this approach, with a goal of widespread adoption by 2007.

The FDA Timeline for RFID Adoption.



The FDA, CBP and the Transportation Security Administration (TSA) are also addressing supply chain security on a global scale with a focus on terrorism. They will ultimately issue guidelines that focus on similar tracking and detection capabilities for all imports. Furthermore, Nevada and Florida have introduced legislation governing electronic pedigrees for pharmaceutical trade at the state level. Life sciences organizations must take the potential regulatory overlaps into account. Counterfeiting impacts several key areas, including:

- ▶ **Consumer Safety:** Most counterfeit drugs are made with no active ingredients and, in some cases, contain dangerous ingredients;
- ▶ **Consumer Confidence:** In the short term, word of mouth associating counterfeiting with a specific medicine can lead to patient anxiety and reduce scripts of key brands. Longer term, it puts strategic investments at risk – reputable brands that may have taken many years and more than a billion dollars to establish;
- ▶ **Sales & Distribution:** As the gray market grows, counterfeits cannibalize sales from authentic medicines. Further, returns and recalls increase the cost of goods sold;
- ▶ **Trade Relationships:** Trading partner relationships will be renegotiated to reflect shared liability. In fact, some leading manufacturers are mandating contracts that prevent selected distributors from buying drugs and devices from anyone except the original manufacturer.

Types of counterfeit drugs.

The World Health Organization (WHO) defines counterfeit drugs as medicines that are deliberately and fraudulently mislabeled with respect to their identities, ingredients and/or sources. There are four basic types of pharmaceutical counterfeits, each presenting unique challenges in terms of detection and response:

- 1) **Identical Copies:** the least common counterfeits are made with the same ingredients, formulas and packaging as originals, but not by the original manufacturer;
- 2) **Look-alikes:** featuring high-quality packaging and convincing appearances, look-alikes contain little or no active ingredients and may be made with harmful substances;
- 3) **Rejects:** actual drugs that have been rejected by the manufacturer for not meeting quality standards;
- 4) **Re-labels:** typically, these authentic drugs have passed their expiration dates or been distributed by unauthorized foreign sources, and may also include placebos created for late-phase clinical trials. The problem reaches beyond medications. More counterfeit medical devices are appearing on the market. Both finished goods and parts have been faked. Typically, they are “look-alike” devices, with high-quality packaging and authentic-seeming appearances, but do not meet medical standards and are not capable of performing intended functions. Examples include everything from aortic pumps to mesh implants for hernia repairs. Counterfeiters have also moved into diagnostic equipment, like stethoscopes and testing systems.

The drivers of counterfeiting.

A \$400 billion-plus industry, pharmaceuticals make a highly attractive target for counterfeiters. It will become even more appealing as new, higher priced drugs enter the market during the next few years. Additionally, the probability of being caught and the resulting penalties are low. For criminals, counterfeiting is easy money.

“The counterfeiters have become more sophisticated as they’ve come to realize that counterfeiting is a good business to get into: it has very low risk of getting caught, very low risk of getting punished severely if you do get caught, and very high reward in terms of profit with low overhead.”

-Darren Pogoda, International Anti-counterfeiting Coalition, January, 2003

Four factors account for the steady increase in pharmaceutical counterfeiting:

- 1) **Computer technology** used to forge labels and other documents is widely available and has become more sophisticated, less costly and easier to use;
- 2) **Increasing numbers of small distributors** buying and selling medications have created a thriving secondary market, also known as the gray market, with medicines meant for relief agencies sometimes diverted by unscrupulous distributors;
- 3) **Growing use of the Internet** to buy medicine has created a very low-cost vehicle for counterfeiters to sell their products, with little or no interference from government regulatory agencies;
- 4) **Increasing prices of premium drugs** make pharmaceuticals an appealing target for criminal organizations, and explain the increasing activity in the U.S., where counterfeiters can command higher prices and generate fatter profits.

Other macroeconomic factors have also played a role, including freer trade, global manufacturing capabilities, lax enforcement and weak intellectual property protection. Drugs that are most often counterfeited are popular high-priced medications, including anti-depressants, statins and AIDS therapies, and drugs with strong brand recognition, like Viagra. The bottom line? In an era of globalized supply chains and truly international markets, the lines between “safe” and “rogue” markets will continue to blur until comprehensive measures are put in place.

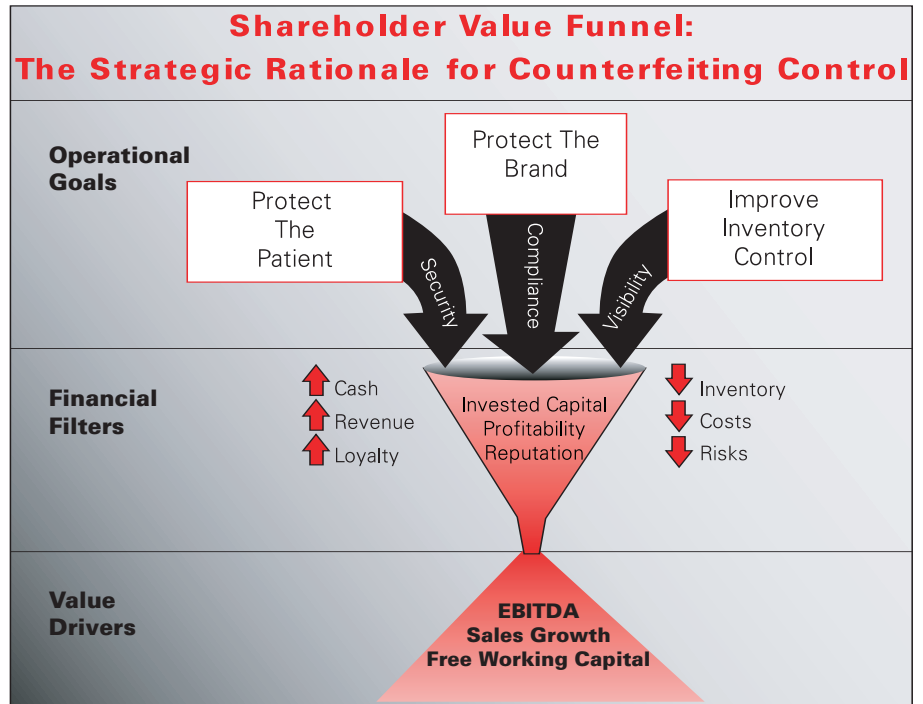
Redefining accountability and performance.

As life sciences executives begin to absorb the potential impact of counterfeits on their research and development investment, their external environment continues to change. First, the concerns over consumer safety are causing the federal government to increase the span of accountability to which it will hold manufacturers. In a recent federal case involving a pharmacist charged with diluting cancer drugs, a major drug manufacturer was named as a codefendant. This is a precedent. Regulatory and liability changes are on the horizon. When investigating counterfeiting, illegal importation and other cases of misuse of branded drugs, regulators typically ask of pharmaceuticals, “What did you know and when did you know it?” Now, they will also ask, “What should you have known?” The standard expectation for awareness will expand to include the operational activities of their trading partners. Answering with “they said they were applying controls” or other “see-no-evil” defenses won't protect pharmaceuticals. Meeting the standard will require monitoring, certification and financial controls.

Second, the market is searching for enhanced shareholder value from manufacturers. To date, the industry has not responded to competitive pressures from generics with the expected degree of innovation and operational excellence. This is creating a bias for action in a historically high-margin, recession-proof sector. Among other things, life sciences manufacturers cannot rely on premium prices to meet EBITDA targets. Further, plans to improve free working capital by exchanging inventory for cash through leaner operations is moving off the whiteboard and into the field. In this environment, executives cannot throw money at the counterfeiting problem without a measurable business justification that goes beyond compliance.

Forward-thinking leaders are seeing the potential for synergy in these twin changes: investing in risk management capabilities also enables improved performance in the operational levers that drive shareholder value.

Unisys is the market leader in delivering in-transit visibility for clients in regulated industries like airlines, public sector and defense.



On the revenue side, legitimate sales will increase as counterfeiting is reduced. Better inventory and asset management will lead to greater stock accuracy, increased inventory turns and an improved order-to-cash cycle time. Optimized relationships with trading partners and increased supply chain visibility will minimize waste, losses and recalls. Better returns management and reduced handling and distribution overhead will drive down costs. Do these benefits represent “easy money” for the industry? No, but they do represent big money, and achieving the benefits is feasible with the right approach.

With large pharmacy operations like Wal-Mart, Target and others mandating that suppliers adopt RFID, pharmaceutical manufacturers should have ample motivation to take a broad view. The involvement of the world’s leading retailers offers further evidence of the cost and efficiency gains to be realized with RFID and related technologies. The Department of Defense (DOD) is also requiring its suppliers to use RFID for tracking and tracing pallets. The bottom line: in nearly every major industry, distributed, RFID-based networks will be critical components of tomorrow’s smart supply chain. That’s why many pharmaceuticals have already been ramping up more advanced logistics and distribution capabilities. Longer term, these advances will also help support the complexity of distributing customized, biotech-style drugs to smaller and more varied patient communities.

The implications for life sciences organizations.

Spending on measures to combat counterfeiting will increase as awareness increases. The spike in spending will be particularly sharp in the area of RFID. Industry analysts are beginning to develop three- to five-year projections. Estimates vary, but it's expected that RFID adoption in the life sciences sector will happen earlier and occur on a larger scale — easily in the hundreds of millions of dollars in the next three years. According to Frost & Sullivan, companies in all industries spent \$1.65 billion on RFID in 2003, with spending expected to increase to \$11.66 billion by 2010. As the anti-counterfeiting capabilities outlined by the FDA are deployed, life sciences organizations will wrestle with a number of challenging questions including:

How will trading partner relationships need to change? The days of arms-length relationships with third-party logistics providers and distributors are over. As drug makers seek to eliminate blind spots, their trading partners will have to strike a new balance between short-term profitability and ongoing risk management. For example, a number of major U.S.-based pharmaceutical manufacturers recently announced they would no longer sell their drugs and devices to U.S. wholesalers who also obtain the manufacturer's products from sources other than the drug makers. In addition, some large distributors see an opportunity to provide manufacturers with value-added services based on information. Smaller, low-cost distributors will face increased scrutiny and may be crowded out by "certified" distributors who can offer increased levels of transparency, security and reliability. According to the FDA and new voluntary guidelines issued by the Healthcare Distribution Management Association (HDMA), appropriate "due diligence" includes "performing background checks, and inspecting the facilities of the potential business partner."

With new drug development requiring an average of 12 years and \$1.7 billion, improving measures to combat counterfeiting should be viewed as guarding a strategic investment.

What to do with all the EPC data? Maintaining drug pedigrees at the item level will tax existing computing infrastructure. Combined with complex handoffs including consolidation and repackaging, the pipeline volume — literally billions of items by node, including dynamic status updates — will stretch existing technical infrastructure. The alerts and notifications from tracking and tracing supply chain events will also challenge management's attention span. The ability to filter essential from non-essential updates will become a strategic capability. Evolving standards for managing shared EPC data across a collaborative network increase complexity. Large distributors may step into the void and offer to serve as data aggregators or consolidators, which could help pharmaceuticals avoid significant costs and complexity. Further, it is not yet clear what role the FDA will play once the infrastructure to support its guidelines is in place. However the data management issues play out, companies should begin planning now for the application of advanced business intelligence and analytical tools. Companies that can figure out how to generate value from this data (e.g., through increased visibility and optimized supply chain performance) will have the opportunity to gain a sustainable competitive edge.

How will existing regulations interact with the new guidelines? For example, while the FDA has issued new guidance around the application of 21 CFR Part 11 regulations, many confusing issues remain. Electronic pedigrees will be subject to some level of validation, but the extent and type of validation are open questions requiring further investigation with the FDA.

Besides electronic pedigrees, where is the biggest “bang for the buck?” What can be done in terms of overt packaging controls and container-level security measures to complement the EPC-based solutions? For example, Optically Variable Microstructures (OVMs), also known as holograms, provide a control that is difficult to duplicate and not dependent on fixed reader devices. Other effective examples are tamper-evident seals and injected chemical signatures.

With all the hype and complexity, where should we start? Backward scheduling the long list of required activities makes it clear that companies simply can't afford to get stuck in the mud if they intend to have robust anti-counterfeiting capabilities by 2007, in accordance with the FDA timeline. Organizations that take a year to evaluate and select the right technologies will probably miss the mark. Technology evaluations are often politicized, leading to indecision and substantial resource drain. They become a threat in their own right. Starting with a solid business case and then proving the value with pilots can be a good strategy, but these initiatives should be based on a proven blueprint of the big picture solution. Further, Unisys recommends that these activities be time-boxed as part of a comprehensive implementation strategy.



RFID: Battle-tested technology.

While many consider RFID a hot new technology, it is actually a proven approach for delivering the highest levels of visibility and security on complex supply chains. As an outcome of the first Gulf War, Unisys partnered with the U.S. Department of Defense to create the world's largest RFID network to track enormous amounts of ordnance, medical supplies and blood moving around the world. The network provides “inside the box” visibility and nodal tracking of equipment and cargo. It is being used successfully during operations in Afghanistan and the second Gulf War.

Unisys has served as the prime integrator and provider of managed services for the Department of Defense's in-transit visibility network since 1994. Consisting of RFID, optical scanning and satellite technologies, the network is deployed in 50+ countries, with more than 750 nodes, including airports, seaports and rail terminals. Currently, it tracks and secures approximately 350,000 conveyances and 25,000 containers every day.

The RFID technology framework.

The technical architecture necessary to meet the FDA's guidelines will be comprised of several components. Today, basic passive RFID tags sell for between \$0.25 and \$0.50 each, with readers in the \$300-\$500 range. Active tags may cost more, depending on their use of micro-sensors, micro-actuators or other nano-technologies. Initial hardware costs will be substantial. The good news is that the cost of these technologies is falling faster than Moore's Law, which dictates that the price is either falling by 50 percent every two years or capability doubles for the same price. Also, most RFID-based applications are proprietary and do not always conform to common technology standards, causing interoperability issues across vendors and systems. To maximize their investment, pharmaceuticals should seek a proven, standards-based portfolio, including:

- ▶ **RFID (Radio Frequency Identification) Tags:** RFID tags incorporate the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal or person. RFID is seeing increased use as an alternative to the bar code. Unlike bar codes, RFID tags do not require a line of sight and can be read automatically at greater distances. RFID tags are capable of transmitting and receiving data, including electronic product codes, and may also contain chip-based micro-sensors capable of detecting physical phenomena (temperature, humidity, toxicity, light, pH, etc.) and micro-actuators that act based on computer instructions to start motors and drives or limit switches. RFID tags communicate with networks and applications through "readers." If stationary, readers can be attached to applications through tethered networks or wireless protocols. If mobile, the readers may be attached directly to applications or through satellite communications. Standards, including the use of the radio frequencies KHz and MHz, are starting to emerge. RFID is the core technical platform for anti-counterfeiting measures based on EPCs.
- ▶ **EPC (Electronic Product Codes):** The electronic product code is the next generation of product identification beyond the UPC or bar code. It is a naming and identification scheme designed to enable the unique identification of physical objects, assemblies and groupings of objects. Consisting of a series of numbers, the EPC can identify the manufacturer, product, version and serial number. Stored in an RFID tag, EPC uses RFID to link to online databases, providing a secure way of sharing product-specific information along the supply chain. EPCs are the keystone for instant verification and drug pedigrees.
- ▶ **PML (Physical Markup Language):** PML is the common language for describing physical objects, physical processes and environments. It acts primarily as a standard communication method between different organizations and databases, communicating information about the state of products tagged with EPCs.

The RFID technology framework relies on distributed network architecture that is shared by supply chain partners. It also includes an integration services layer that synthesizes disparate information formats used by devices in the field. The integration services must conform to EPC standards in order to effectively support communities of supply chain partners. By applying analytics and business intelligence tools, data about adverse supply chain events is culled from the integration services layer and transformed into alerts and notifications. These messages are presented to operations managers using performance dashboards that classify and prioritize exceptions.

Complementing the RFID technology framework are a number of new packaging strategies, including electronic ink, holograms, tamper-proof wrappings and dynamic displays that can be activated with electronic charges. These can be applied to pallets, cases or individual packages.

The path forward — creating a chain of custody.

In general, the term “chain of custody” refers to a process used to maintain and document a chronological history of evidence. Applied to counterfeiting, it refers to combining electronic and physical capabilities to create situational awareness about an item's past and future as it moves through the supply chain. The electronic capabilities blend automated authentication (e.g., “instant verification”) with EPC tracking (Where is the item now? Where is it going?) and electronic pedigrees (Where has the item been?). The physical capabilities like CCTV used to monitor dock-to-stock processes and smart container seals create “zero gap” safety zones where variability or “blind spots” can reliably be eliminated from the equation.

Creating a chain of custody for medicines and medical devices requires a broad view. Although the priorities shift over time, a comprehensive solution will maintain visibility throughout an item's entire life cycle, even as raw and semi-finished materials change form and cross borders prior to the finished goods manufacturing process. No single countermeasure will ensure safety across the board. Throughout the journey, three types of controls are necessary:

1) information-based, 2) relationship-based, and 3) physical. With these controls in mind, life sciences organizations should focus on a few key success areas when developing secure supply chain solutions: prevention, detection, response and infrastructure.

Prevention: There is much manufacturers can do to prevent counterfeiting before it happens, including the implementation of both direct and indirect controls. Employee vetting and zone-controlled facility access are examples of direct, physical controls that can help prevent counterfeiting at specific sites or by specific trading partners. Direct controls can also be relationship-based, including distributor and carrier certification programs where compliance with standards is a condition for ongoing business. Indirect controls are not site-specific and are designed to deter counterfeiting by the criminal community in general. Examples include manufacturer-mandated contracts that force distributors to buy only from authorized suppliers and financial strategies like trusted agent payment systems that link distributor compensation to security certification and performance. Furthermore, information controls like assessment of trading partner profiles and patterns provide clues for proactive investigation.

Detection: Detection pertains to finding counterfeits that have already been introduced into the pipeline. One of the largest barriers to effective detection has historically been the availability of affordable automated inspection technology. EPC-based verification has the potential to solve this problem. EPC verification is highly reliable and requires little or no manual processing. However, the effectiveness of EPC-based verification is only as good as the physical security around it. That is, instant verification works only if physical procedures and processes force all items to pass by readers prior to reaching the consumers.

There can be no doubt that information-based detection control has great potential value in the near term and will clearly be a pillar of optimum patient safety in the future, but the implementation challenges are numerous and complex. Taking it to the next level with electronic drug pedigrees will require the use of more robust track and trace capabilities. Cross-organization integration requirements mean that partners in the life sciences value chain will need a lot of practice before large-scale implementations can occur. The synchronization of dynamic data, agreement on standards and the risk of “false positives” are notable challenges here. Analytical tools and techniques will help address these challenges by filtering the explosion of EPC data and distilling it to meaningful patterns and exceptions.

The effectiveness of EPC-based verification is only as good as the physical security around it.

Detecting counterfeits at the package level is a primary goal, but it is not the only goal. Container-level security is another critical element. For example, item-level scans may be performed as trucks are loaded at the distributor, but, depending on channels, it may not be possible to scan items again before they reach consumers. After all, in the real world, it will be some time before all retail pharmacies adopt RFID or EPC, and thus not all drugs that reach patients will undergo EPC verification. In this case, the ability to verify that individual containers have been loaded securely and not been opened during trips provides a very valuable control. Manufacturers must collaborate with carriers, freight forwarders and distributors to improve both physical and technical controls at the container level. Securing goods on the move at the container level, though less precise than item-level tracking, yields a compelling return for the cost.

Response: Response controls are standardized actions that are triggered when counterfeiting threats are detected or suspected. Currently, there are limited guidelines as to what action to take when counterfeits are detected, and the information is incomplete about the scope of counterfeiting for a particular drug. The FDA guidelines will help drive better information and guidance, though life sciences organizations should seize the opportunity and actively participate in the FDA's efforts to improve response controls. They should also seek the input of their trading partners. Among the best practices likely to emerge include maintaining single points of contact regarding counterfeiting for each trading partner (relationship); decisive and highly visible response to exceptions that are detected in the chain of custody — with trading partners frequently notified that the counterfeiting threat is being actively monitored (information/relationship); and standard processes for notifying the relevant law enforcement agencies (information). It's clear that the FDA (and other agencies) will play a role in this area. The sooner life sciences organizations can engage the agency and understand their evolving point of view, the better their future needs will be served.

Ensuring the authenticity and security of the tens of billions of items flowing through the life sciences pipeline will tax the capabilities of technical and human networks.



Infrastructure: Infrastructure is the final key success area in a comprehensive anti-counterfeiting program. Ensuring the authenticity and security of the tens of billions of items flowing through the life sciences pipeline will tax the capabilities of technical and human networks. PML — a common language for describing physical objects (like a bottle of medicine) — will play a key enabling role. The FDA guidelines imply the need for a distributed network far exceeding anything previously attempted in the life sciences arena. As if the installation and implementation challenges were not enough, such a network will create significant business continuity issues such as information security, constant availability and disaster recovery. Further, there are the “blue collar” tasks such as field service, maintenance and help desk support. The information infrastructure will be a complex mix of multiple services, technologies, applications and platforms. RFID capabilities, both the passive and active variety, will underpin solutions, though their use will vary depending on the supply chain segment in question. Applications created to support track and trace capabilities and drug pedigrees will need to comply with previous regulations regarding electronic records.

Conclusions.

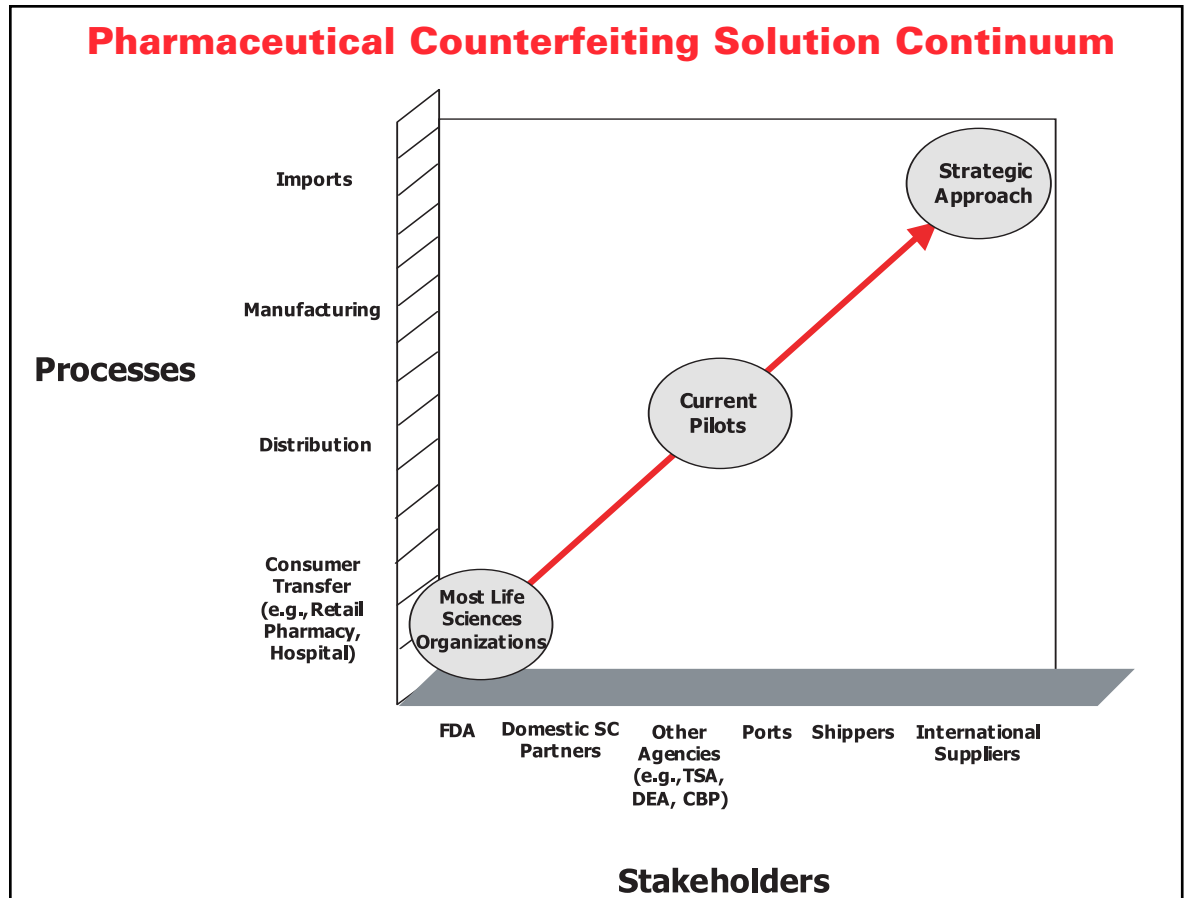
Recognize the strategic value. The FDA has, more or less, pushed the cost of figuring out how to stop counterfeiting on to industry. A significant investment in people, relationships and infrastructure is required. But the synergies inherent in the increased visibility needed to combat counterfeiting enable a broad spectrum of value. For example, Unisys research suggests that the typical large pharmaceutical manufacturer can expect to realize significant financial returns through a successfully deployed chain of custody including:

- ▶ 15 to 20 percent reduction in inventory levels;
- ▶ seven to 10 percent reduction in costs;
- ▶ four to six percent increase in customer (physician) retention.

A chain of custody also enables consistency with regulatory guidelines and retailer programs, which will ultimately mitigate compliance risks. Finally, in an industry where patient safety is the cornerstone of all activity, a chain of custody has boardroom relevance regardless of shifting business conditions.

Think beyond the pilot. Some industry partners are already investigating anti-counterfeiting strategies through working groups and collaborative pilots. The hype cycle is in full swing and there is significantly more talking than doing. Many of these pilots focus on sorting through the technology questions between domestic manufacturer and retail pharmacy. This is necessary thinking but it is not sufficient. The bigger picture implications stemming from the global supply chain are a blind spot in many of these efforts. Furthermore, these pilots offer limited insight into the realities of operating a high-volume, highly secure network based on an open distributed infrastructure. Understanding how to manage these and other complexities should be a near-term priority for executives looking to achieve meaningful benefits from a chain of custody.

Pharmaceutical Counterfeiting Solution Continuum



While some providers devise “point solutions” addressing individual aspects of supply chain security, Unisys Guardian Anti-Counterfeiting Solutions address the entire life cycle.

Why Unisys?

Unisys is the market leader in delivering in-transit visibility for clients in regulated industries like airlines, public sector and defense. Combined with our life sciences industry experience and insight, our track record implementing “zero-gap” security solutions makes Unisys the safe partner to support all aspects of your anti-counterfeiting program – from strategy to ongoing operations. For example, we partnered with the Department of Defense to implement and manage the largest RFID-enabled supply chain visibility solution in the world. We manage the air cargo supply chain for major airlines and are the IT security service provider for 249 airports. We are leading four projects for the TSA’s Operation Safe Commerce program, which is designed to improve container security for U.S. imports. We have a global life sciences practice and active engagements with three of the top five global pharmaceutical manufacturers, as well as the FDA. Unisys Guardian Anti-Counterfeiting Solutions for life sciences are comprehensive solutions based on real experience in the field. They minimize risk and time-to-benefit. Our dedicated teams of experienced supply chain and life sciences specialists use a proven 3D Blueprinting approach. The blueprints are based on reusable code and process templates designed to accelerate solution delivery. 3D Blueprinting allows clients to start their anti-counterfeiting programs “with the end in mind.”

***For further information, visit
www.safecommerce@unisys.com or
contact Unisys Life Sciences at
1.800.874.8647 x424.***

Specifications are subject to change without notice.

© 2004 Unisys Corporation

All rights reserved.

Unisys is a registered trademark of Unisys Corporation.

All other brands and products referenced herein are acknowledged to
be trademarks or registered trademarks of their respective holders.

Printed in US America 4/04



41364332-000